

# Anonymisation avancée de données multimodales en santé: vers des garanties mathématiques de non-réversibilité

## Contexte

Les start-ups en santé numérique manipulent des données hautement sensibles : enregistrements vocaux, rapports cliniques textuels et données issues de la vision par ordinateur.

Les entreprises en santé numérique font face à un enjeu central : comment exploiter ces données pour développer des outils cliniques innovants tout en garantissant une protection robuste de la vie privée des patients.

Ainsi, au-delà des exigences réglementaires standards, ces entreprises cherchent à développer des méthodes d'anonymisation avancées permettant :

- une **protection robuste de la vie privée des patients**,
- un maintien de la qualité des données pour une utilisation clinique,
- une **réutilisation secondaire des données** (recherche, entraînement de modèles),
- et le maintien d'une **pertinence clinique**.

Cette problématique est particulièrement critique dans le contexte :

- de l'entraînement de modèles d'intelligence artificielle,
- de la réutilisation secondaire des données à des fins de recherche,
- de la collaboration interinstitutionnelle,
- et des exigences réglementaires croissantes (HIPAA, Loi 25, RGPD, etc.).

Certaines modalités sont intrinsèquement riches en informations identifiantes :

- la voix contient une signature biométrique unique,
- le texte clinique libre peut révéler des informations personnelles ou contextuelles,
- Les composantes linguistiques, le contenu, les thématiques, ainsi que les composantes paralinguistiques peuvent faciliter une ré-identification directe ou indirecte,
- les images et vidéos peuvent permettre une ré-identification directe ou indirecte,
- et les données multimodales croisées augmentent fortement les risques de ré-identification.

Le projet vise donc à développer des approches mathématiques et algorithmiques avancées permettant de concevoir des mécanismes d'anonymisation robustes, transférables et compatibles avec les besoins réels des environnements cliniques.

## Problématique

Comment concevoir des méthodes d'anonymisation pour des données multimodales qui soient :

1. **Mathématiquement garanties comme non réversibles** (ou quantifiables en termes de risque de ré-identification) ?

2. **Utiles pour des tâches cliniques** (classification, détection, suivi, soutien à la décision clinique, analyse prédictive, entraînement de modèle IA) malgré la transformation des données ?
3. **Généralisables à des contextes de faible volume de données**, en exploitant éventuellement des données publiques, au transfert d'apprentissage ou synthétiques ?
4. **Suffisamment qualitatives pour assurer une augmentation potentielle des données et une utilisation secondaire.**
5. **Interopérables et transférables à différents milieux cliniques et types de données (audio, texte, image, questionnaires, données comportementales) ?**

### Axes de recherche proposés

Les participants sont invités à explorer des approches combinant outils de mathématiques appliquées, statistique, optimisation et apprentissage automatique :

- **Mesures de confidentialité** : formalisation du risque via des cadres comme la confidentialité différentielle ou des métriques informationnelles (entropie, information mutuelle).
- **Transformations non réversibles** : conception d'opérateurs (stochastiques ou déterministes)
- **Apprentissage de représentations anonymisées** : utilisation de techniques issues de l'apprentissage profond pour produire des embeddings invariants à l'identité.
- **Données synthétiques** : génération de jeux de données réalistes via modèles probabilistes ou génératifs (GANs, modèles de diffusion) avec garanties de confidentialité.
- **Évaluation multi-objectif** :
  - performance sur tâches cliniques,
  - robustesse face à des attaques de ré-identification,
  - interprétabilité et acceptabilité.

### Défis mathématiques

- Établir des **bornes théoriques** sur la ré-identification à partir de données transformées.
- Comprendre les **compromis fondamentaux** entre utilité et anonymisation.
- Concevoir des **algorithmes efficaces en régime de petites données.**
- Intégrer plusieurs modalités (audio, texte, image) dans un cadre unifié.
- Développer des approches robustes en contexte de petits échantillons de données.
- Évaluer les risques liés aux attaques modernes de reconstruction ou d'inférence.

### Données

Selon les disponibilités :

- jeux de données réels fournis (anonymisés partiellement),
- données publiques,
- ou données synthétiques générées pour les besoins du projet.

## Retombées attendues

- Méthodes d'anonymisation avec **garanties quantifiables**.
- Outils transférables aux start-ups partenaires.
- Contributions théoriques et algorithmiques à l'intersection de la statistique, de l'optimisation et de l'apprentissage.

## Pourquoi participer ?

Ce projet se situe au cœur de problématiques sociétales majeures : **protection de la vie privée, IA responsable, et innovation en santé**. Il offre un terrain riche pour mobiliser des outils mathématiques avancés tout en ayant un impact concret.

## Compagnies partenaires du projet

### FLOW

Flow est une entreprise québécoise en santé numérique développant une plateforme clinique intelligente destinée aux professionnels de la santé mentale et des disciplines connexes. Sa mission est de soutenir les cliniciens dans la gestion, la structuration et l'analyse de l'information clinique complexe grâce à une intégration responsable de l'intelligence artificielle.

La plateforme vise à améliorer l'efficacité des processus cliniques et administratifs tout en préservant l'autonomie professionnelle, le jugement clinique et la qualité de la relation thérapeutique. Elle permet notamment de centraliser des données multimodales provenant de différentes sources cliniques, telles que des questionnaires, des notes textuelles, des documents, des données comportementales et d'autres informations pertinentes au suivi des patients.

### Phonia

Phonia est une entreprise québécoise en santé numérique ayant développé une reconnaissance vocale de pointe pour le domaine de l'orthophonie, de la santé de la communication, du langage, de la parole et de l'apprentissage. Son modèle de reconnaissance vocale automatique permet une analyse clinique des corpus de langage et de parole nécessaire pour la réalisation des activités cliniques des orthophonistes. En plus d'une transcription automatisée et une analyse fine des corpus, ce scribe IA spécialisé au domaine de la parole, de la voix et du langage pathologiques est inclus au sein d'une plateforme complémentaire de services d'Intelligence Artificielle permettant la facilitation de la pratique orthophonique allant de la tenue des dossiers professionnels, à la rédaction des documents professionnels (rapports professionnels, collecte et rédaction de compte-rendu d'anamnèse), tout en passant par l'aide à la prise de décision et l'aide à la génération de matériel thérapeutique.